REMARKS

A. Claims 1 and 222-28 have been amended to put into better for, remove any issues which may arise under 35 .S.C. §112, paragraph 2, and to positively include patentable features into the body of the claims(s).

B. Claims 1 and 22-28 were rejected under 35 U.S.C. §103(a) as being unpatentable over Holloway et al. (US 5,805,801) in view of Sofer et al. (US 5,489,896) and in further view of Sherer (US 5,935,245). The applicant respectfully traverses this rejection for the following reason(s).

Holloway's invention relates to systems and methods for detecting and preventing intrusion into a campus local area network (LAN) by an unauthorized user. A managed hub discovers each interconnect device in the network that supports the security feature and maintains an interconnect device list of such devices, which may include token ring switches, Ethernet switches, bridges and routers. The managed hub determines the interconnect devices in the campus network that are capable of supporting a local area network (LAN) security feature. The managed hub then uses the responses to build and maintain a table of interconnect devices in the network that support the security feature. Here, during a discovery phase, the managed hub periodically sends a discovery frame to a LAN security feature group address. The managed hub detects an intrusion by an unauthorized address on one of its ports by comparing the MAC addresses on each port against a list

of authorized MAC addresses, disables the port and notifies the other interconnect devices in the network of the intrusion by transmitting a security breach detected frame to the LAN security feature group address. The interconnect devices set a filter on their respective ports against the intruding unauthorized address.

Sofer's invention relates to a security unit for a network having a data bus to which a plurality of stations (interconnect devices) can be connected wherein the security unit monitors traffic on the data bus and only enables authorized data to flow along the data bus. The data bus and the security unit are part of a hub. The traffic includes a multiplicity of data packets each having source and destination addresses and the security unit includes a plurality of correlators for determining that the source and destination addresses indicate an authorized communication. Additionally, each station is connected to the data bus via a port having a port address and one of the correlators correlates the source address with an authorized port address.

Note that Sofer's port address is not the same nor equivalent to a destination address, as Sofer clearly differentiates the two addresses. A destination address is the final destination for the message, where the port address is for a particular port connected to the final destination.

Sofer differs from Holloway in that Sofer teaches the destination station address be in a list of authorized destination station addresses for the source station address, because Sofer is concerned with permitting two stations being authorized to communicate with each other. Holloway is only concerned with **intrusion** by an unauthorized source station outside the network breaking into the network via one of the ports. There is no concern with whether a source station is authorized to connect to a destination station.

Sherer's invention relates to a method and apparatus for providing secure network communications on a per-packet level in a network system. According to Sherer, adaptor cards or drivers for installation in a network include a simple data pattern enforcer (DPE) operating at the lowest layer at which packets are recognized. The DPE may be comprised of hardware or software elements and have associated with it a mechanism for applying a rule or a set of rules to packets either transmitted or received at the lowest layer at which the packets exist. These mechanisms may include a set of one or more pattern-matching masks and a count indication into the packet as to where pattern-matching will begin.

Up to three values are used by the data pattern enforcer (DPE): a Count, a Value Bit Vector (VBV), and a Don't Care Bit Vector (DCBV). The count is a value indicating a position in a network data packet. For example, the count may represent a number of bytes into a network packet. The VBV is a bit string that is compared to the bits in the packet at the position indicated by the count. The DCBV, if present, is a mask indicating whether or not certain bit locations within the VBV are values that are not used by the matching. If a DCBV is used, for every bit in the VBV there is a Don't Care Bit (DCB) indicating whether that bit is used or ignored in the compare.

For example, if VBV=01101110, DCBV=10000001 and Count=4 , then when a packet is received off the network, the byte indicated by the count is examined. The data pattern enforcer (DPE) expects the data to be of the format x110111x, where x indicates don't-care bit positions (either 0 or 1) and the other values match what is in a VBV register. The examined byte may be a byte in a packet header, either part (source or destination) of a MAC address, the IPX address, or the IP address. However, Sherer's invention allows verification to happen at any place in the packet as determined by the count value.

The present invention has an advantage over the applied art, because of its use of access vectors. An access vector has been defined by the specification to consist of a bit vector. The bit value "0" means restriction to access and "1" means allowance for access. For example, if a server node S1 has an access vector 00010000 and a client node C1 has access vector 10000001, then client node (source station) C1 cannot access server node (destination station) S1, but another client node C2 having access vector 00010001 can access server node S1.

For further understanding, access vector 00010000 of a server node S1 means that S1's HostID is 3, and its access vector is 0x80>>3. If C1 is going to be an access client node, the access vector of C1 should be (0x80>>3). If the access vector of C1 is 10010001, then this access vector 10010001 means C1 can access server nodes that have HostID 0, 3 or 7. Thus a client node having an access vector xxx1xxxx (x can be a 0 or 1) can access a server node having a HostID of 3, and a client node having an access vector xxx0xxxx (x can be a 0 or 1) is restricted from accessing a server node having a HostID of 3.

Accordingly, it is possible to use the same (e.g., 8-bit) access vectors for more than one (32-bit) source address and (32-bit) destination address, thereby saving memory space for storing the correlating 8-bit access vectors instead of correlating each 32-bit source address and destination address.

Claim 1

Claim 1, as amended, is directed to a MAC (media access control) address-based communication restricting method using **access vectors stored in address tables**, wherein the access

vectors indicate whether two nodes, corresponding to a MAC source address and a MAC destination address, may access each other, the method calls for, in part:

detecting, in the an address table, access vectors corresponding to the MAC destination and source addresses, wherein the access vectors are stored in address tables and indicate whether two nodes, corresponding to a MAC source address and a MAC destination address, may access each other.

The combination of applied art fails to teach the foregoing feature.

Contrary to the Examiner's remarks, neither Holloway nor Sofer teach *access vectors*, much less *access vectors stored in address tables*. The Examiner is respectfully requested to identify where the phrase "access vectors" is found in both Holloway and Sofer.

Note that the phrase "access vectors" are defined by the specification, and it is an error for the Examiner to give them a different definition. During examination, the claims must be interpreted as broadly **as their terms reasonably allow**. This means that the words of the claim must be given their plain meaning **unless applicant has provided a clear definition in the specification**. See MPEP §2111.01; and *Toro Co. v. White Consol. Indus., Inc.*, 199 F.3d 1295, 1299, 53 USPQ2d 1065, 1067 (Fed. Cir. 1999)("[W]ords in patent claims are given their ordinary meaning in the usage of the field of the invention, unless the text of the patent makes clear that a word was used with a special meaning.").

- In the final rejection, the Examiner states that the phrase "access vector" has been given the broadest reasonable interpretation in light of the specification. Yet, the Examiner goes on to state

that claim 1 does not define what an access vector specifically is, and that there is only a cursory discussion in the preamble, not the body of the claim.

Note that it is not required that the claim define what an access vector is as long as the text of the patent makes clear that a word was used with a special meaning (See *Toro Co. v. White Consol. Indus., Inc.*, supra) **and** the words of the claim must be given their plain meaning **unless applicant has provided a clear definition in the specification** (See MPEP §2111.01).

Accordingly, both the MPEP and the cited case law (*Toro*) indicate that the claim does not need to define "access vector" since it is defined in the specification. Additionally, MPEP § 2173.05(a)(I), which states, when the specification states the meaning that a term in the claim is intended to have, the claim is examined using that meaning, in order to achieve a complete exploration of the applicant's invention and its relation to the prior art. *In re Zletz*, 893 F.2d 319, 13 USPQ2d 1320 (Fed. Cir. 1989).

Additionally, although Sherer does teach a Value Bit Vector (VBV), this VBV is not an access vector stored in an address table, but instead is an 8-bit value stored in a register. See Fig. 6, registers 95 and 95a of rule sets 98 and 98a, respectively.

Accordingly, Sherer does not teach *access vectors stored in address tables*.

Therefore, the rejection of claim 1 is deemed to be in error and should be withdrawn.

The VBV in Sherer is simply an 8-bit value that should appear somewhere (corresponding

to a stored count value stored in a count register 93 or 93a of rule sets 98 and 98a, respectively) in a received data packet. According to the count value, a byte of received data corresponding to the location identified by the count value is compared with the VBV to determine if the received packet should be discarded or received.

Claim 1 requires that a MAC destination address and a MAC source address included in the received packet data be read, and that the access vectors corresponding to the MAC destination and source addresses the address table be detected. Upon detection of **both** the access vector corresponding to the MAC destination address and the access vector corresponding to the MAC source address. Then the access vector corresponding to the MAC destination address is compared to the access vector corresponding to the MAC source address. The two nodes (preamble), corresponding to the MAC source address and the MAC destination address are denied access to each other if the access vectors of the MAC destination and source addresses are not matched.

Sherer does not teach comparing two VBV's to each other.

Sherer does not teach comparing an access vector corresponding to a received MAC destination address to an access vector corresponding to a received MAC source address, i.e., *reading a MAC destination address and a MAC source address included in the received packet data;* and *detecting, in the address table, access vectors corresponding to the MAC destination and source addresses.*

Sherer does not teach *denying* [two nodes] *access* [to each other] *if the access vectors of the MAC destination and source addresses are not matched.* See preamble and last feature of claim 1.

Instead Sherer teaches accepting or rejecting a received data packet.

- In the final rejection the Examiner indicates the system of Holloway compares incoming MAC addresses with the destination MAC address (referring to col. 8, lines 1-14) to see if they are able to communicate based on the filter.

We note that this is not what is disclosed or taught by Holloway. Instead, Holloway discloses comparing a source address (the last source address on a port (an apparent intruder)) with an authorized list of MAC addresses (the list having been defined for this port). Col. 8, lines 12.

Holloway is unconcerned with MAC destination addresses, and is only concerned with MAC source addresses at a particular port.

- The Examiner argues it would have been obvious to one ordinary skilled in the art at the time the invention was made to modify Holloway's invention with the teachings of Sofer to include a MAC stripper to extract the MAC destination and source addresses from the received packets. One would be motivated to do so in order to provide the system with ability to determine where did the packet come form and where the packet is headed to and if it's headed to a protected destination.

Note however, that in Holloway, all destinations are protected. Holloway's invention relates to systems and methods for detecting and preventing intrusion into a campus local area network by an unauthorized user. Accordingly the campus, and more particularly, the local area network of the campus is protected. An authorized list of source MAC addresses is defined for each port in a managed hub. The managed hub detects an intrusion by an unauthorized source MAC address on one of its ports by comparing the source MAC addresses on each port against a list of authorized source MAC addresses, disables the port and notifies the other interconnect devices in the network

of the intrusion by transmitting a security breach detected frame to the LAN security feature group address. The interconnect devices set a filter on their respective ports against the intruding unauthorized source MAC address.

Accordingly, Holloway determines where a packet comes from and is not concerned with where the packet is headed.

Neither Sofer nor Sherer would have suggested to one of ordinary skill in the art that Holloway need be concerned with where the packet was headed, *i.e.,* the source MAC address.

Therefore, there is not motivation to combine the teaching of Sofer and Sherer with the teaching of Holloway, as no advantage in doing so will be achieved.

Uniroyal, Inc. v Rudkin-Wiley Corp., 837 F.2d 1044, 5 USPQ2d 1434 (Fed. Cir. 1988) states: "Something in the prior art as a whole must suggest the desirability, and thus the obviousness, of making the combination"; and cites *Lindemann Maschinenfabrik GmbH v. American Hoist and Derrick Co.,* 730 F.2d 1452, 1462, 221 USPQ 481, 488 (Fed. Cir. 1984), which cites *In re Imperato,* 486 F.2d 585, 179 USPQ 703 (CCPA 1973) and *In re Sernaker,* 702 F.2d 989, 217 USPQ 1 (Fed. Cir. 1983) which states: "prior art references in combination do not make an invention obvious unless something in the prior art references would suggest the advantage to be derived from combining their teachings."

Therefore, the rejection of claim 1 is deemed to be in error and should be withdrawn.

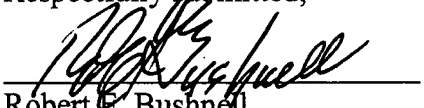
Further, the Applicant has asserted that the use of access vectors instead of MAC destination

and source addresses for comparison is advantageous over the art. The Examiner has not addressed the asserted advantage. See MPEP §707.07(f).

Claims 22-28 are deemed to be non-obvious and patentable over the art of record for the same reasons as claim 1.

The Examiner is respectfully requested to reconsider the application, withdraw the objections and/or rejections and pass the application to issue in view of the above amendments and/or remarks.

Respectfully submitted,



Robert E. Bushnell
Attorney for Applicant
Reg. No.: 27,774

1522 K Street, N.W.
Washington, D.C. 20005
(202) 408-9040

Folio: P56339
Date: 10/12/07
I.D.: REB/MDP